

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1 Claims 1.-9. (canceled).

1 Claim 10. (currently amended) A method performed by a custodian computing
 2 system, having memory, to share a secret S among n secret owners such that any k of the n secret
 3 owners may reconstruct the secret S , the method comprising the steps of:

4 choosing two large primes P and Q , such that PQ is greater than S when S is a
 5 number;

6 ~~computing, at the custodian computing system, and storing in the custodian~~
 7 ~~computer system memory a product $N = PQ$;~~

8 ~~computing and storing a product $M = (P-1)(Q-1)$;~~

9 choosing n random numbers e_1 through e_n that are relatively prime to N ;

10 choosing another random number e that is relatively prime to N ;

11 choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \leq i \leq n$;

12 choosing another number d such that $ed \bmod M$ is equal to one;

13 ~~generating and storing a database of $\binom{n}{k}$ values, where each value is the product~~

14 ~~of d and a unique k of the d_i numbers for $1 \leq i \leq n$, wherein each value is associated with a~~
 15 ~~unique combination of k secret owners of the n secret owners;~~

16 storing a database of $\binom{n}{k}$ entries, wherein each entry is associated with a unique

17 combination of the $\binom{n}{k}$ possible combinations of the k secret owners, and wherein a particular

18 entry includes a value, c , that is the product of modulus M of d and the d_i values for i indices that

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

19 correspond to the particular secret owners present in the unique combination for that particular
 20 entry, wherein c corresponds to modulus M of the product kdi :
 21 computing S^c ;
 22 deleting from the custodian computer memory P , Q , and M ;
 23 computing S^c ;
 24 distributing n secret owner pieces to each of the n secret owners, wherein each of
 25 the secret owner pieces includes S^c and one of the numbers e_1 through e_n ;
 26 deleting the secret S and e_1 through e_n , d_1 through d_n , and d ;
 27 receiving k secret owner values from a unique combination of k secret owners;
 28 determining a the value c that is associated with the unique combination; and
 29 determining the secret S using the value c retrieved from the database entry
 30 corresponding to the k secret owners whose secret owner pieces have been received and the k
 31 secret owner values and $S^c \bmod N$.

1 Claim 11. (previously presented) A method as in claim 10, wherein receiving k
 2 secret owner values from the unique combination of k secret owners comprises:
 3 receiving a first of the n secret owner pieces from one of the n secret owners; and
 4 computing and storing $S' = S^{ef} \bmod N$, where f represents the one of the numbers
 5 e_1 through e_n contained in the first of the n secret owner pieces.

1 Claim 12. (previously presented) A method as in claim 11, wherein receiving k
 2 secret owner values from the unique combination of k secret owners comprises:
 3 receiving a second of the n secret owner pieces from another one of the n secret
 4 owners;
 5 computing $S^q \bmod N$, where q represents the one of the numbers e_1 through e_n
 6 contained in the second of the n secret owner pieces; and replacing S' with $S^q \bmod N$.

1 Claim 13. (previously presented) A method as in claim 12, wherein receiving k
 2 secret owner values from the unique combination of k secret owners comprises:

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

3 each time another of the secret owner pieces is received from another one of the
 4 secret owners;
 5 computing $S^q \bmod N$, where q represents the one of the numbers e_1 through e_n
 6 contained in the another of the n secret owner pieces; and replacing S' with $S^q \bmod N$.

1 Claim 14. (previously presented) A method as in claim 13, further comprising
 2 the steps of:

3 after k secret owner pieces have been received,
 4 retrieving from the database the value c from among the $\binom{n}{k}$ values, wherein the
 5 value c corresponds to the k secret owner pieces of the unique combination of k secret owners
 6 that were received by the custodian;
 7 computing $S^c \bmod N$; and
 8 replacing S' with $S^c \bmod N$.

1 Claim 15. (currently amended) A method performed by a custodian computing
 2 system, having memory, to share a secret S among n secret owners such that any k of the n secret
 3 owners may reconstruct the secret, the method comprising the steps of:

4 choosing two large primes P and Q , such that PQ is greater than S where S is a
 5 number;
 6 ~~computing, at the custodian computing system, and~~ storing in the custodian
 7 computer memory a product $N = PQ$;
 8 ~~computing and~~ storing a product $M = (P-1)(Q-1)$;
 9 choosing n random numbers e_1 through e_n that are relatively prime to N ;
 10 choosing random numbers e and e' that are relatively prime to N ;
 11 choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \leq i \leq n$;
 12 choosing numbers d and d' such that $ed \bmod M$ is equal to one and such that $e'd'$
 13 $\bmod M$ is equal to one;

Appl. No. 09/853,913
 Amtd. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

14 ~~generating and storing a database of $\binom{n}{k}$ values, where each value is the product~~
 15 ~~of d and a unique k of the d_i numbers for $1 \leq i \leq n$, wherein each value is associated with a~~
 16 ~~unique combination of k secret owners of the n secret owners;~~
 17 storing a database of $\binom{n}{k}$ entries, wherein each entry is associated with a unique
 18 combination of the $\binom{n}{k}$ possible combinations of the k secret owners, and wherein a particular
 19 entry includes a value, c , that is the product of modulus M of d and the d_i values for i indices that
 20 correspond to the particular secret owners present in the unique combination for that particular
 21 entry, wherein c corresponds to modulus M of the product $k d_i$;
 22 computing $S^{ee'}$;
 23 deleting from the custodian computer memory P , Q , and M ;
 24 computing $S^{ee'}$;
 25 distributing n secret owner pieces to each of the n secret owners, wherein each of
 26 the secret owner pieces includes $S^{ee'}$ and one of the numbers e_1 through e_n ;
 27 deleting the secret S and e_1 through e_n , d_1 through d_n , and d
 28 receiving k secret owner values from a unique combination of k secret owners;
 29 determining retrieving from the database a the value c that is associated with the
 30 unique combination; and
 31 determining the secret S using the value c and the k secret owner value.

1 Claim 16. (previously presented) A method as in claim 15, wherein receiving k
 2 secret owner values from the unique combination of k secret owners comprises:
 3 receiving a first of the n secret owner pieces from one of the n secret owners; and
 4 computing and storing $S' = S^{ee'f} \bmod N$, where f represents the one of the numbers
 5 e_1 through e_n contained in the first of the n secret owner pieces.

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

1 Claim 17. (previously presented) A method as in claim 16, wherein receiving k
 2 secret owner values from the unique combination of k secret owners comprises:
 3 receiving a second of the n secret owner pieces from another one of the n secret
 4 owners;
 5 computing $S^q \bmod N$, where q represents the one of the numbers e_1 through e_n
 6 contained in the second of the n secret owner pieces; and replacing S' with $S^q \bmod N$.

1 Claim 18. (previously presented) A method as in claim 17, wherein receiving k
 2 secret owner values from the unique combination of k secret owners comprises:
 3 each time another of the secret owner pieces is received from another one of the n
 4 secret owners;
 5 computing $S^q \bmod N$, where q represents the one of the numbers e_1 through e_n
 6 contained in the another of the n secret owner pieces; and replacing S' with $S^q \bmod N$.

1 Claim 19. (previously presented) A method as in claim 18, further comprising
 2 the steps of:
 3 after k secret owner pieces have been received,
 4 retrieving from the database the value c from among the $\binom{n}{k}$ values, wherein the
 5 value c corresponds to the k secret owner pieces from the unique combination of k secret owners
 6 that were received by the custodian;
 7 computing $S^c \bmod N$;
 8 replacing S' with $S^c \bmod N$;
 9 computing $S^{d'} \bmod N$; and
 10 replacing S' with $S^{d'} \bmod N$.

1 Claim 20. (currently amended) A method performed by a custodian computing
 2 system, having memory, to share a secret among n secret owners such that any k of the n secret
 3 owners may reconstruct the secret, the method comprising the steps of:

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

4 encrypting the secret so as to generate an encrypted secret;
 5 deleting from the custodian computer memory the secret; and
 6 performing a forward k out of n secret sharing algorithm on the encrypted secret
 7 so as to generate n secret owner pieces;
 8 storing in a database a plurality of ~~values~~ entries associated with a plurality of
 9 unique combinations of k secret owners of the n secret owners, wherein a particular entry
 10 includes a value, c , that is the product of modulus M of d and the d_i values for i indices that
 11 correspond to the particular secret owners present in the unique combination for that particular
 12 entry, wherein c corresponds to modulus M of the product kdi ;
 13 distributing the n secret owner pieces to the n secret owners;
 14 receiving k secret owner values from a unique combination of k secret owners;
 15 ~~determining~~ retrieving from the database a value c that is associated with the
 16 unique combination;
 17 performing a reverse k out of n secret sharing algorithm on the k secret owner
 18 pieces so as to recreate the encrypted secret using the value c ; and
 19 decrypting the encrypted secret so as to recreate the secret.

Claims 21. - 24. (canceled).

1 Claim 25. (original) A method as in claim 20, wherein the step of performing a
 2 forward k out of n secret sharing algorithm includes the steps of:
 3 dividing the encrypted secret into k pieces; and
 4 performing n polynomial evaluations at n points of a degree- k polynomial using
 5 the k pieces of the encrypted secret as polynomial coefficients;
 6 wherein each of the k secret owner pieces includes a result of one of the n
 7 polynomial evaluations and a corresponding one of the n points.

1 Claim 26. (previously presented) A method as in claim 25, wherein the step of
 2 performing a reverse k out of n secret sharing algorithm includes the steps of generating a system

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

3 of k linear equations and solving the system of k linear equations for the k pieces of the encrypted
 4 secret.

1 Claim 27. (previously presented) A method as in claim 26, further comprising
 2 the step of:
 3 assembling the k pieces of the encrypted secret so as to recreate the encrypted
 4 secret.

Claims 28.-29. (canceled).

1 Claim 30. (currently amended) A computer readable storage medium having
 2 embodied thereon computer readable program code suitable for programming a computer to
 3 perform a method performed by a custodian to share a secret S among n secret owners such that
 4 any k of the n secret owners may reconstruct the secret, the method comprising the steps of:
 5 choosing two large primes P and Q , such that PQ is greater than S where S is a
 6 number;
 7 computing and storing a product $N = PQ$;
 8 computing and storing a product $M = (P-1)(Q-1)$;
 9 choosing n random numbers e_1 through e_n that are relatively prime to N ;
 10 choosing another random number e that is relatively prime to N ;
 11 choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \leq i \leq n$;
 12 choosing another number d such that $ed \bmod M$ is equal to one;
 13 generating and storing a database of $\binom{n}{k}$ values, where each value is the product
 14 of d and a unique k of the d_i numbers for $1 \leq i \leq n$, wherein each value is associated with a
 15 unique combination of k secret owners of the n secret owners;

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

16 storing a database of $\binom{n}{k}$ entries, wherein each entry is associated with a unique
 17 combination of the $\binom{n}{k}$ possible combinations of the k secret owners, and wherein a particular
 18 entry includes a value, c, that is the product of modulus M of d and the d_i values for i indices that
 19 correspond to the particular secret owners present in the unique combination for that particular
 20 entry, wherein c corresponds to modulus M of the product $k d_i$;
 21 computing S^e ;
 22 deleting P, Q, and M;
 23 computing S^e ;
 24 distributing n secret owner pieces to each of the n secret owners, wherein each of
 25 the secret owner pieces includes S^e and one of the numbers e_1 through e_n ;
 26 deleting the secret S and e_1 through e_n , e, d_1 through d_n , and d;
 27 receiving k secret owner values from a unique combination of k secret owners;
 28 determining retrieving from the database one of the a values c that is associated
 29 with the unique combination; and
 30 determining the secret S using the value c and the k secret owner values.

1 Claim 31. (currently amended) A computer readable storage medium having
 2 embodied thereon computer readable program code suitable for programming a computer to
 3 perform a method performed by a custodian to share a secret S among n secret owners such that
 4 any k of the n secret owners may reconstruct the secret, the method comprising the steps of:
 5 choosing two large primes P and Q, such that PQ is greater than S where S is a
 6 number;
 7 computing and storing a product $N = PQ$;
 8 computing and storing a product $M = (P-1)(Q-1)$;
 9 choosing n random numbers e_1 through e_n that are relatively prime to N;
 10 choosing random numbers e and e' that are relatively prime to N;

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

11 choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \leq i \leq n$;
 12 choosing numbers d and d' such that $ed \bmod M$ is equal to one and such that $e'd'$
 13 $\bmod M$ is equal to one;
 14 generating and storing a database of $\binom{n}{k}$ values, where each value is the product
 15 of d and a unique k of the d_i numbers for $1 \leq i \leq n$, wherein each value is associated with a
 16 unique combination of k secret owners of the n secret owners;
 17 storing a database of $\binom{n}{k}$ entries, wherein each entry is associated with a unique
 18 combination of the $\binom{n}{k}$ possible combinations of the k secret owners, and wherein a particular
 19 entry includes a value, c , that is the product of modulus M of d and the d_i values for i indices that
 20 correspond to the particular secret owners present in the unique combination for that particular
 21 entry, wherein c corresponds to modulus M of the product kdi ;
 22 computing $S^{ee'}$;
 23 deleting P , Q , and M ;
 24 ~~computing $S^{ee'}$;~~
 25 distributing n secret owner pieces to each of the n secret owners, wherein each of
 26 the secret owner pieces includes $S^{ee'}$ and one of the numbers e_1 through e_n ;
 27 deleting the secret S and e_1 through e_n , d_1 through d_n , and d ;
 28 receiving k secret owner values from a unique combination of k secret owners;
 29 ~~determining~~ retrieving from the database one of the a values c that is associated
 30 with the unique combination; and
 31 determining the secret S using the value c and the k secret owner values.

1 Claim 32. (currently amended) A computer readable storage medium having
 2 embodied thereon computer readable program code suitable for programming a computer to

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

perform a method performed by a custodian to share a secret among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

- encrypting the secret so as to generate an encrypted secret;
- deleting the secret;
- performing a forward k out of n secret sharing algorithm on the encrypted secret so as to generate n secret owner pieces;
- storing in a database a plurality of values entries associated with a plurality of unique combinations of k secret owners of the n secret owners, wherein a particular entry includes a value, c , that is the product of modulus M of d and the d_i values for i indices that correspond to the particular secret owners present in the unique combination for that particular entry, wherein c corresponds to modulus M of the product $k d_i$;
- distributing the n secret owner pieces to the n secret owners;
- receiving k secret owner values from a unique combination of k secret owners;
- ~~determining~~ retrieving from the database one of the a values c that is associated with the unique combination;
- performing a reverse k out of n secret sharing algorithm on the k secret owner pieces so as to recreate the encrypted secret using the value c ; and
- decrypting the encrypted secret so as to recreate the secret.

Claims 33.-34. (canceled).

Claim 35. (currently amended) A computer comprising a processor and a computer readable storage medium coupled to the processor having embodied thereon processor readable program code suitable for programming a computer to perform a method performed by a custodian to share a secret S among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

- choosing two large primes P and Q , such that PQ is greater than S where S is a number;
- ~~computing and storing~~ a product $N = PQ$;
- ~~computing and storing~~ a product $M = (P-1)(Q-1)$;

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

10 choosing n random numbers e_1 through e_n that are relatively prime to N ;
 11 choosing another random number e that is relatively prime to N ;
 12 choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \leq i \leq n$;
 13 choosing another number d such that $ed \bmod M$ is equal to one;
 14 ~~generating and storing a database of $\binom{n}{k}$ values, where each value is the product~~
 15 ~~of d and a unique k of the d_i numbers for $1 \leq i \leq n$, wherein each value is associated with a~~
 16 ~~unique combination of k secret owners of the n secret owners;~~
 17 storing a database of $\binom{n}{k}$ entries, wherein each entry is associated with a unique
 18 combination of the $\binom{n}{k}$ possible combinations of the k secret owners, and wherein a particular
 19 entry includes a value, c , that is the product of modulus M of d and the d_i values for i indices that
 20 correspond to the particular secret owners present in the unique combination for that particular
 21 entry, wherein c corresponds to modulus M of the product $k d_i$;
 22 computing S^e ;
 23 deleting P , Q , and M ;
 24 computing S^e ;
 25 distributing n secret owner pieces to each of the n secret owners, wherein each of
 26 the secret owner pieces includes S^e and one of the numbers e_1 through e_n ;
 27 deleting the secret S and e_1 through e_n , e , d_1 through d_n , and d ;
 28 receiving k secret owner values from a unique combination of k secret owners;
 29 determining retrieving from the database one of the values c that is associated
 30 with the unique combination; and
 31 determining the secret S using the value c and the k secret owner values.

1 Claim 36. (currently amended) A computer comprising a processor and a
 2 computer readable storage medium coupled to the processor having embodied thereon processor

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

readable program code suitable for programming the computer to perform a method performed by a custodian to share a secret S among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

choosing two large primes P and Q , such that PQ is greater than S where S is a number;

~~computing and storing a product $N = PQ$;~~

~~computing and storing a product $M = (P-1)(Q-1)$;~~

choosing n random numbers e_1 through e_n that are relatively prime to N ;

choosing random numbers e and e' that are relatively prime to N ;

choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \leq i \leq n$;

choosing numbers d and d' such that $ed \bmod M$ is equal to one and such that $e'd' \bmod M$ is equal to one;

generating and storing a database of $\binom{n}{k}$ values, where each value is the product of d and a unique k of the d_i numbers for $1 \leq i \leq n$, wherein each value is associated with a unique combination of k secret owners of the n secret owners;

storing a database of $\binom{n}{k}$ entries, wherein each entry is associated with a unique

combination of the $\binom{n}{k}$ possible combinations of the k secret owners, and wherein a particular

entry includes a value, c , that is the product of modulus M of d and the d_i values for i indices that correspond to the particular secret owners present in the unique combination for that particular entry, wherein c corresponds to modulus M of the product $k d_i$;

computing $S^{ee'}$;

deleting P , Q , and M ;

~~computing $S^{ee'}$;~~

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes $S^{ee'}$ and one of the numbers e_1 through e_n ;

Appl. No. 09/853,913
 Amdt. dated May 22, 2006
 Reply to Office Action of December 21, 2005

PATENT

28 deleting the secret S and e_1 through e_n , d_1 through d_n , and d ;
 29 receiving k secret owner values from a unique combination of k secret owners;
 30 ~~determining~~ retrieving from the database one of the a values c that is associated
 31 with the unique combination; and
 32 determining the secret S using the value c and the k secret owner values.

1 Claim 37. (currently amended) A computer comprising a processor and a
 2 computer readable storage medium coupled to the processor having embodied thereon processor
 3 readable program code suitable for programming the computer to perform a method performed
 4 by a custodian to share a secret among n secret owner such that any k of the n secret owners may
 5 reconstruct the secret, the method comprising the steps of:
 6 encrypting the secret so as to generate an encrypted secret;
 7 deleting the secret;
 8 performing a forward k out of n secret sharing algorithm on the encrypted secret
 9 so as to generate n secret owner pieces;
 10 storing in a database a plurality of values entries associated with a plurality of
 11 unique combinations of k secret owners of the n secret owners, wherein a particular entry
 12 includes a value, c , that is the product of modulus M of d and the d_i values for i indices that
 13 correspond to the particular secret owners present in the unique combination for that particular
 14 entry, wherein c corresponds to modulus M of the product $k d_i$;
 15 distributing the n secret owner pieces to the n secret owners;
 16 receiving k secret owner values from a unique combination of k secret owners;
 17 ~~determining~~ retrieving from the database one of the a values c that is associated
 18 with the unique combination;
 19 performing a reverse k out of n secret sharing algorithm on the k secret owner
 20 pieces so as to recreate the encrypted secret using the value c ; and
 21 decrypting the encrypted secret so as to recreate the secret.